Arizona State Senate
Issue Paper

December 1, 2006

Note to Reader:

The Senate Research Staff provides nonpartisan, objective legislative research, policy analysis and related assistance to the members of the Arizona State Senate. The *Research Briefs* series, which includes the *Issue Brief, Background Brief* and *Issue Paper*, is intended to introduce a reader to various legislatively related issues and provide useful resources to assist the reader in learning more on a given topic. Because of frequent legislative and executive activity, topics may undergo frequent changes. Additionally, nothing in the *Brief* should be used to draw conclusions on the legality of an issue.

IDENTITY THEFT AND CONSUMER PROTECTION

INTRODUCTION

Identity theft and identity fraud are terms used to refer to all types of crimes in which someone wrongfully obtains and uses another person's personal information such as a name, Social Security number (SSN), credit card number or other identifying information to commit fraud or deception, typically for economic gain.

Identity theft is one of the fastest growing crimes in the United States and is a large problem in Arizona. The Phoenix/Mesa metropolitan area continually is ranked as an area with the highest per capita rate of identity theft. The most common identity theft complaints relate to credit card fraud, phone or utilities fraud, bank fraud and employment-related fraud. According to the Federal Trade Commission (FTC), complaints from Arizonans relating to employment-related fraud are more than double what they are in all other locations in the United States.

According to the Department of Justice's Bureau of Justice Statistics, in 2004, 3.6 million households, or three percent of all households, discovered during the past six months that at least one member of the household was a victim of identity theft. The estimated loss as a result of identity theft reported by the victimized households was about $3.2 billon. Additionally, about one-third of households victimized by any type of identity theft report that problems associated with the theft were resolved in one day; about one-fifth of households spent two to seven days; and about one-fifth of households spent one month or more.

In May 2006, President George W. Bush created an Identity Theft Task Force to develop a comprehensive national strategy to combat identity theft. In September 2006, the Task Force made seven interim recommendations. Generally, the Task Force's recommendations related to data breach guidelines for governmental agencies, data security, governmental response to data breaches, developing a universal police report for identity theft victims, allowing federal identity theft victims to recover for the value of the time that they spent attempting to rectify the identity theft, reducing access to SSNs and developing alternative methods for authenticating an individual's identity.

IDENTITY THEFT

Federal law prohibits knowingly transferring or using, without lawful authority, a means of identification of another person with the intent to commit, or to aid and abet, any unlawful activity that constitutes a violation of federal law or that constitutes a felony under any applicable state or local law. State laws relating to identity theft vary in the definition of the offense.

In Arizona, identity theft is defined as knowingly taking, purchasing, manufacturing, recording, possessing or using any personal identifying information or entity identifying information of another person or entity, including a real or fictitious person or entity, without the consent of that other person or entity, with the intent to obtain or use the other person's or entity's identity for any unlawful purpose or to cause loss to a person or entity whether or not the person or entity actually suffers any economic loss as a result of the offense. Arizona classifies identity theft as a class 4 felony (A.R.S. § 13-2008).

Arizona also penalizes other acts of identity theft. Aggravated identity theft, a class 3 felony, occurs when a person commits identity theft that results in an economic loss of $3,000 or more or commits identity theft against five or more persons or entities (A.R.S. § 13-2009). Additionally, trafficking in identities is penalized as a class 2 felony (A.R.S. § 13-2010). The identity theft statutes do not apply to persons under the age of 21 utilizing fake identifications for buying or consuming alcohol or being admitted to an over-21 venue. Arizona law also protects against identity theft by protecting against credit card fraud (Title 13, Chapter 21).

PROTECTING YOUR SSN

A SSN is a unique personal identifier issued by the government to an individual and, in today's computer age, is relied upon as a unique identifier for administrative and verification purposes. Since one SSN is assigned to one person, government agencies and businesses use them to identify and track service use.

While there is no federal law that universally addresses the use of SSNs by public and private entities, there are several federal laws that address the use and disclosure of SSNs by specific industries. For example, the Social Security Number Confidential Act of 2000 prohibits the appearance of SSNs on or through unopened mailings of checks or other drafts issued on public money in the Treasury.

The Intelligence Reform and Terrorism Prevention Act of 2004, applicable to documents issued after December 17, 2005, restricts the issuance of replacement Social Security cards to three per year and ten in a lifetime, and establishes minimum standards for verification of documents submitted to establish eligibility for Social Security cards. It also prohibits any government from displaying SSNs or any derivative on driver licenses, motor vehicle registrations or other identification documents issued by any department of motor vehicles.

Arizona law universally addresses the use of SSNs. While an individual may always elect to have the SSN printed on a document (A.R.S. § 44-1373), several laws protect an individual from undesired SSN disclosure.

Arizona law prohibits a person or entity from making an individual's SSN available to the general public. This includes postings to public websites without a password, insecure Internet transmission, cards used to receive public services and mailed items, with some exceptions. This law does not apply to SSN uses that were in place prior to January 1, 2005, if certain steps are taken, such as providing the individual with an annual written disclosure informing of the right to stop such disclosure of the SSN (A.R.S. § 44-1373). Furthermore, beginning January 1, 2009, a person or entity may not knowingly print any sequence of more than five numbers that are reasonably identifiable as part of an individual's SSN on any card required to receive products or services or on any materials mailed to the individual, with certain exceptions (A.R.S. § 44-1373.02).

Beginning January 1, 2007, documents or records that are recorded and made available on an entity's public website must not contain more

than five numbers that are identifiable as part of the person's SSN (A.R.S. § 44-1373).

Statute allows state agencies to use or disseminate the last four digits of an individual's SSN (A.R.S. § 44-1373); however, the Department of Revenue and state and local law enforcement agencies are authorized to utilize the full number with some exceptions (A.R.S. § 44-1373.01). Statute also allows the use of SSNs by state agencies for the administration of payroll and workers' benefits with some exceptions (A.R.S. § 44-1373.01).

The attorney general or a county attorney may commence a legal action for a violation of the SSN use statutes (A.R.S. § 44-1373).

In addition to those statutes pertaining directly to SSNs, some other statutes limit the use of SSNs by specific entities. The education statutes prohibit a university from assigning an individual identification number that is identical to the individual's SSN and require a community college to assign an identification number different from the SSN upon request. Additionally, a university or community college may not display any four or more consecutive numbers of an individual's SSN on any university Internet site or other publicly accessible document. Schools may still electronically transfer student transcripts to other schools (A.R.S. § 15-1823).

Furthermore, the Arizona Department of Real Estate prohibits the release of a licensee's SSN for inspection by any person other than the court or a government agency (A.R.S. § 32-2125.03); and any employee of the Department of Economic Security (DES) who discloses personal information, including a SSN, collected by DES for a specified purpose without authorization may be subject to a $1,000 civil penalty, in addition to other sanctions (A.R.S. § 23-722.01).

OTHER ARIZONA LAWS AIMED AT PROTECTING CONSUMERS AGAINST IDENTITY THEFT

Security Breach

In February 2005, ChoicePoint, a corporation that collects and compiles consumer information, including personal and financial information, disclosed that it had been the victim of a security breach. In this case, personal identifying information of approximately 145,000 people was sold to a criminal enterprise. At first, the corporation only disclosed of the breach to California residents, as required by California state law. However, the corporation later disclosed that residents in other states may have been affected by the security breach. Numerous other breaches of security at corporations, government agencies and educational institutions have since been reported, such as breaches at Card Systems, Western Illinois University and the United States Department of Veterans Affairs. These instances have led many states, including Arizona, to enact legislation requiring that companies and/or state agencies disclose to consumers information about security breaches of personal information.

Beginning January 1, 2007, a person, business or governmental entity conducting business in Arizona that owns or licenses unencrypted computerized data that includes personal information and becomes aware of an incident of unauthorized acquisition of, and access to, unencrypted or unredacted computerized data is required to conduct an investigation to promptly determine if a security breach has occurred. Personal information is defined as a person's first name or first initial and last name in combination with the individual's SSN, driver license or nonoperating identification license, or financial account number or credit or debit card number with the required access code. These notification requirements apply to a natural person, business entity or a governmental entity. If the person or entity determines that a security breach has occurred, the person is required to notify the affected Arizona residents.

Notification must be made in the most expedient manner possible without unreasonable delay subject to the needs of law enforcement. The notification is required to be made either in written, electronic or telephonic means or provided by a substitute notice if specified requirements are met (A.R.S. § 44-7501).

It is important to note that a breach in security that may result in personal identifying information being obtained does not necessarily mean that person whose information may have been accessed is a victim of identity theft. Rather, security breach notification is a precaution to alert consumers that their personal information has been breached and they should closely monitor their consumer activity.

Destruction of Documents

Recent concerns have mounted about entities disposing of records that may contain personal information. Consumers are fearful that "dumpster divers" may obtain their personal information from discarded records and use it to commit identity theft. Therefore, the Arizona Legislature enacted mandatory procedures for the destruction of documents.

A business or governmental entity is prohibited from knowingly discarding or disposing of paper records or paper documents without redacting the information or destroying the records or documents if they contain an individual's first and last name or first initial and last name in combination with a corresponding complete:

1. SSN.
2. credit card, charge card or debit card number.
3. retirement account number.
4. savings, checking or securities entitlement account number.
5. driver license number or nonoperating identification license number (A.R.S. § 44-7601).

Also, in response to concerns that personal information, which could be used to commit identity theft, was inadvertently available to the public after a consumer transaction, state law requires that no more than the last five digits of a credit card account number or the credit card expiration date may be printed on the credit card receipt provided to the cardholder if the receipt is electronically printed. A violation is a violation of the Consumer Fraud Act (A.R.S. § 44-1367).

Documents Obtained by Governmental Entities

Many documents are recorded with various governmental entities. With the advent of the Internet, many of these documents now are posted online. In order to protect consumers' personal information, beginning January 1, 2007, it is prohibited to record to a public website documents or records that contain any of the following personal identifying information of an Arizona resident: 1) more than five digits of a SSN; 2) credit card, charge card or debit card numbers; 3) retirement account numbers; or 4) savings, checking or securities entitlement account numbers. The Attorney General or a county attorney, or both, may initiate legal action for a violation. There is a civil penalty of up to $500 for each act of recording personal identifying information, but statute limits the penalties to the person or entity that authorizes the creation of the documents for recording (A.R.S. § 44-1373).

Additionally, government agencies are required to establish procedures ensuring that collected entity identifying information and personal identifying information, except public records, cannot be accessed by unauthorized persons (A.R.S. § 41-4172).

Pretexting

According to the Federal Trade Commission (FTC), pretexting is the practice of obtaining personal information under false pretenses. Pretexters sell personal identifiers to others who may use it to obtain credit in another person's name, steal assets or investigate or sue another person. As an example, data brokers have fraudulently gained access to telephone records by posing as the customer, then offering the records for sale on the Internet without the customer's consent or knowledge.

A person is prohibited from knowingly procuring, selling or receiving a telephone record of any Arizona resident without the resident's authorization. Additionally, telephone companies must establish reasonable procedures to protect against unauthorized or fraudulent disclosure of telephone records. Any violation

of the telephone record requirements is a violation of the Consumer Fraud Act and is a class 1 misdemeanor. For a civil action, a person is entitled to receive at least $1,000 in damages, appropriate relief and reasonable attorney's fees and costs (A.R.S. §§ 44-1376 to 44-1376.05).

Protections on the Internet

Phishing is a form of online identity theft that uses spoofed electronic mail messages (emails) designed to lure recipients to fraudulent websites that attempt to trick them into divulging personal financial data such as credit card numbers, account usernames passwords, and SSNs.

In Arizona, solicitation of an individual's identifying information via a web page or email by a person falsely representing an online business is prohibited and is a class 5 felony. The Attorney General or a person who either is engaged in the business of providing Internet access service to the public or owns a web page or trademark and who is adversely affected by the unauthorized solicitation may institute an action against the violator to stop them from conducting any further phishing and/or to recover actual damages or $500,000 for each separate violation, whichever is greater. The court may increase the damage award up to three times for an established pattern and practice of unauthorized solicitation (A.R.S. §§ 44-7201 to 44-7204).

According to the FTC, computer software known as spyware is installed on a computer without the person's consent. The spyware software monitors or controls computer use. It can be used to send pop-up ads, redirect a computer to particular websites, monitor Internet surfing or record keystrokes, which, in turn, could lead to identity theft. In October of 2004, the FTC filed its first spyware case against a company, alleging the company acted unfairly in downloading software without any notice or authorization that modified the web browser to change consumers' home pages and search engines and that downloaded additional software that caused harm to consumers

In Arizona, it is unlawful for a person to transmit spyware to a computer the person does not own or operate in order to modify, through intentionally deceptive means, computer software or settings or to collect personal identifying information of the computer owner or operator. The spyware statutes preempt all rules, regulations, codes, ordinances and other laws adopted regarding spyware, and the Attorney General and others may bring action against a person who violates the computer spyware provisions to recover the greater of actual damages or $100,000 for each separate violation. The court may increase the damages up to three times the allowed amount if a pattern and practice of violating the provisions can be established (A.R.S. §§ 44-7301 to 44-7304).

As more people use email, marketers are increasingly using email to advertise their products and services. In many cases, the advertisers are sending unsolicited commercial email (UCE), also known as unsolicited bulk mail, junk mail or spam. In a study conducted by the FTC, it was found that approximately 86 percent of the addresses posted to web pages received spam as did 86 percent of the addresses posted to newsgroups. The FTC found that "spammers" obtain email addresses by buying lists from brokers who have "harvested" addresses from Internet newsgroup postings, chat rooms, websites and online services members' directories. The spammers are then able to send thousands, and even millions, of email at one time.

The use of UCE is regulated in Arizona. The transmission of commercial emails that contain false information regarding the origin of the message or content is prohibited. The first characters on the subject line of a UCE must be the characters "ADV." A person who sends UCE or maintains a database for the purpose of sending UCE must provide a free procedure for recipients to remove themselves from the sender's email address list and must restrict the future sale of their email address information. The sender of UCEs is allowed three business days to remove a recipient's email address from the list.

The following is permitted, however: 1) commercial emails to be sent if there is an established business relationship; 2) damages to be collected by a person or email service provider if injured as a result of intentional transmission of UCE; and 3) establishment and enforcement of an email service provider's company policies to block the receipt or transmission of commercial email advertisements that it believes are sent or will be sent in violation of the law. It is a class 2 misdemeanor to violate the statutes governing commercial email (A.R.S. §§ 44-1372 to 44-1372.05).

Additionally, unsolicited faxes have been common. In Arizona, each unsolicited commercial fax advertisement is required to include the name, address, fax number and toll free or local contact telephone number of the vendor that sends the fax. A person who receives unsolicited commercial faxes from a vendor after requesting that no further faxes be sent may charge the vendor $5 for each faxed page received after a three-day grace period. This does not alter or restrict the rights of a person to recover damages for the sending of an unsolicited commercial fax advertisement under federal law (A.R.S. § 44-1482).

ADDITIONAL RESOURCES

- Federal Trade Commission
  www.consumer.gov/idtheft
- National Consumer Protection Week, Identity Theft
  www.consumer.gov/ncpw/index.htme
- Phoenix Police Department, Identity Theft
  http://phoenix.gov//POLICE/dcd1.html
- Maricopa County Attorney's Office, Arizona Identity Theft Statistics
  www.maricopacountyattorney.org/specialized_prosecution/identity_theft/id_theft_stats.html
- National Conference of State Legislatures
  www.ncsl.org/programs/lis/privacy/idtheft.htm
- Arizona Motor Vehicle Division (to remove an SSN from a driver's license)
  http://www.azdot.gov/mvd/index.asp
- U.S. Social Security Administration
  www.socialsecurity.gov
- U.S. General Accounting Office
  www.gao.gov
- Free annual credit report from each company
  www.annualcreditreport.com
- Equifax
  www.equifax.com
- TransUnion
  www.transunion.com
- Experian
  www.experian.com
- National Do Not Call Registry
  www.donotcall.gov
- FTC website on Spam
  http://www.ftc.gov/spam/
- Consumer Sentinel
  http://www.consumer.gov/sentinel/
- The Driver's Privacy Protection Act of 1994: 18 U.S.C. §§ 2721 to 2725
- Fair and Accurate Transaction Act of 2003: 15 U.S.C. §§ 1681 *et seq.*; 20 U.S.C. §§ 9701 *et seq.*
- Fair Credit Reporting Act: 15 U.S.C. §§ 1681 *et seq.*
- The Gramm-Leach Bliley Act of 1999: 12 U.S.C. §§ 24a, 248b, 1820a, 1828b, 1831v to 1831y, 1848a, 2908, 4809; 15 U.S.C. §§ 80b-10a, 6701, 6711 to 6717, 6731 to 6735, 6751 to 6766, 6781, 6801 to 6809, 6821 to 6827, 6901 to 6910
- The Health Insurance Portability and Accountability Act of 1996: 18 U.S.C. §§ 24, 669, 1035, 1347, 1518, 3486; 26 U.S.C. §§ 220, 4980C to 4980E, 6039F, 6050Q, 7702B, 9801 to 9806; 29 U.S.C. §§ 1181 to 1187; 42 U.S.C. §§ 300gg, 300gg-11 to 300gg-13, 300gg-21 to 300gg-23, 300gg-41 to 300gg-47, 300gg-91, 300gg-92, 1320a-7c

to 1320a-7e, 1320d, 1320d-1 to 1320d-8, 1395b-5, 1395ddd

- Identity Theft Penalty Enhancement Act: 18 U.S.C. §§ 1028 *et seq.*
- Arizona Forgery and Related Offenses, including Identity Theft, Statutes: A.R.S. Title 13, Chapter 20
- Arizona Credit Card Statutes: A.R.S. Title 13, Chapter 21
- Arizona Internet Representations Statutes: A.R.S. Title 44, Chapter 29
- Arizona Confidentiality of Personal Identifying Information Statutes: A.R.S. Title 44, Chapter 9, Article 17